DOCUMENT RESUME

ED 473 378 EA 032 397

| | |
|---|---|
| AUTHOR | Strang, Kirk D. |
| TITLE | Technology in Public Education: What Will the Quest for Fairness and Efficiency Do to Individual Interests and Rights? |
| PUB DATE | 2002-11-00 |
| NOTE | 17p.; In: Balancing Rights: Education Law in a Brave New World. Papers [of the] Education Law Association (ELA) Annual Conference (48th, New Orleans, LA, November 14-16, 2002); see EA 032 361. |
| PUB TYPE | Information Analyses (070) -- Speeches/Meeting Papers (150) |
| EDRS PRICE | EDRS Price MF01 Plus Postage. PC Not Available from EDRS |
| DESCRIPTORS | *Appropriate Technology; Civil Liberties; Crime Prevention; Discipline Policy; Disclosure; Educational Technology; Elementary Secondary Education; *Privacy; *Public Education; School Law; *School Responsibility; *School Security; School Supervision; Student Rights; Teacher Rights |
| IDENTIFIERS | *Electronic Surveillance; Employee Rights; *Monitoring |

ABSTRACT

This paper—part of a collection of 54 papers from the 48th annual conference of the Education Law Association held in November 2002—is an outline of a presentation on monitoring the activities of students and school personnel. The dilemma, according to this paper, is that public schools are obliged to prevent persons under their supervision from causing harm to others. Yet satisfying such responsibilities increasingly requires more active, and sometimes intrusive, means of supervising and monitoring the activities of students and school personnel. The first section of the outline describes the nature of the dilemma. The next section examines events and factors that may influence public perceptions of schools' responsibilities. The next section discusses legal duties that can encourage heightened supervision and monitoring. The next section examines relevant legal authority and includes analyses of litigation involving employee polygraph protection and privacy rights and technology. The next section presents negligence theories that may affect schools' use of monitoring technology. The final section discusses the use of technology to monitor student and employee activities, touching upon monitoring of email and Internet usage, video surveillance cameras, and metal detectors. (WFA)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 473 378

# Technology in Public Education: What Will the Quest for Fairness and Efficiency Do to Individual Interests and Rights?

Kirk D. Strang

November 2002

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

✔ This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality

• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL IN MICROFICHE, AND IN ELECTRONIC MEDIA FOR ERIC COLLECTION SUBSCRIBERS ONLY, HAS BEEN GRANTED BY

R. Wagner

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

2A

BEST COPY AVAILABLE

EA 032 397

# TECHNOLOGY IN PUBLIC EDUCATION: WHAT WILL THE QUEST FOR FAIRNESS AND EFFICIENCY DO TO INDIVIDUAL INTERESTS AND RIGHTS?

Kirk D. Strang
Davis & Kuelthau, s.c.
Ten E. Doty, Ste. 600
P.O. Box 1068
Madison, WI 53701-1068

EA032397

I. **NATURE OF THE DILEMMA**: Public schools have to satisfy a variety of legal duties to prevent persons under their supervision from causing actionable harm to others. Sometimes, these responsibilities are mandated by force of law; sometimes they are driven by public expectations and perceptions. These duties implicate any number of services provided by public school districts, including the districts' roles as educators, employers, and caregivers. Yet satisfying these responsibilities (or, just as often, addressing related liability exposure issues) increasingly requires more active, and sometimes more intrusive means of monitoring the activities of employees and pupils. Further, school districts (and others) have greater technological means available to them to monitor the activities of others. As a result, as technology and other means of supervising and monitoring others' activities improves, the legal argument that schools can take or should have taken additional steps to prevent harm that may follow from those activities improves with it.

II. **EVENTS AND FACTORS THAT MAY INFLUENCE PUBLIC PERCEPTIONS OF SCHOOLS RESPONSIBILITIES**

A. **Columbine High School**: The tragic events at this Colorado high school stimulated a national discussion on school safety. The public's search for answers and its determination that events such as this must not be repeated prompted many to ask whether schools can do more to identify students who are or may become dangerous. This concern contributes to the public's expectation that schools should do more than punish wrongdoing, but should also gather intelligence to prevent harm from occurring in the first place.

B. **September 11, 2001**: The terrorist hijackings and bombing of the World Trade Center caused the nation to question whether accepted security measures can be relied on to provide for public safety and whether further compromises on privacy are essential to protect the public. In the months following the attacks, federal authorities were increasingly called upon to account for their intelligence prior to the attacks, and to establish that the attacks could not have been prevented.

C. **The Child Abductions Of 2002**: Although the impact of the past summer's events is not entirely clear (nor is it certain whether this phenomenon was statistically significant or a function of media reporting practices), parental fears have been exacerbated by the seemingly endless series of assaults, and compounded even further by the disquieting circumstances of certain cases (where children were abducted in or just outside of their homes). Parents' expectations that schools will police their facilities and will have painstakingly investigated employees' backgrounds will likely be even higher than before in light of these events. Moreover, the public tends to assume that information that is acquired by or is available through government sources is provided to or is easily obtained by other governmental authorities. As a result, the public is often surprised (to the

point that it believes governmental authorities have been asleep at the switch) when one governmental entity, such as a school district, is not aware of information that another governmental agency, such as a law enforcement agency, has at its disposal regarding an individual or group.

D. **Public Perceptions Of The Resources and Capabilities Of Public Schools**: Many school officials view the last ten years as a time of limited resources and difficult budgetary decisions. However, the public at large often believes that public schools have considerable resources. Further, school officials generally report that the public believes that schools have a far greater capacity to supervise employees and pupils than may, in fact, be the case.

E. **Sexual Harassment Laws (And Other Employment Laws)**: As a general matter, schools will be required to take reasonable steps to prevent harassment, provide effective means for employees to seek relief, and take prompt remedial action when misconduct is found. In order to prevail, employment attorneys bringing actions against school districts must successfully assign responsibility to the school district for conduct that is often difficult for the district to detect in the absence of an affirmative report. As a result, plaintiffs of necessity must focus on what the employer did not do, and claim that if such steps had been taken, the harm at issue would not have occurred.

F. **The Definition Of "Privacy"**: Conventional understandings of "privacy" are not always consistent with established legal principles on the subject. Monitoring through technological means (as well as other forms of monitoring and surveillance) is permissible in a variety of circumstances. This means that schools often cannot raise the defense that monitoring would have been an unlawful invasion of privacy and may have to defend a decision not to monitor particular communications, a failure to consider monitoring altogether, or a failure to apply more invasive monitoring protocols which, if done, would allegedly have detected the offending conduct and placed the school district in a position to stop it. This problem is compounded by the fact that school districts often place students and staff on notice that certain forms of communication are not private and may be monitored, heightening the expectation that prophylactic monitoring will occur.

## III. LEGAL DUTIES THAT CAN ENCOURAGE HEIGHTENED SUPERVISION AND MONITORING:

A. **Pupil Discipline**: School districts generally have broad authority to sanction pupil conduct that poses a danger to others and, again generally speaking, conduct that is considered dangerous


BEST COPY AVAILABLE

includes a variety of behavior. Thus, although school districts generally are inclined toward remediation (in order to continue to provide educational and support services to students that present discipline problems), school districts are under increasing pressure to remove offenders from the student population through suspension or expulsion, and understand that their failure to do so will likely result in claims that the district failed to take steps that were well within its power to prevent harm to third persons.

B. **Title IX**: School districts can be held liable in certain circumstances for, e.g., one pupil's harassment of another pupil, provided that the district showed deliberate indifference to the offending conduct. Because it is often difficult for claimants to prove that this standard has been satisfied with the proverbial "smoking gun" (e.g., proof that express complaints were systematically disregarded), claimants are increasingly resorting to proof that districts are deliberately choosing not to employ means at their disposal which, if used, would have prevented the conduct in question.

C. **Negligence Principles**: (negligent hiring, supervision, and retention): Negligence principles implicate almost every aspect of a school district's operations, from parking lot supervision to background checks of job applicants. Generally, negligence principles will require that a school district exercise due care to prevent foreseeable harm. The public has high expectations (sometimes unreasonably so) that school districts can control that conduct of all persons under their supervision or in their facilities, and appears to treat most conduct as foreseeable and preventable. Technological means of supervision are often "required" by the demands of the public and the specter of litigation, given the availability of technological remedies, its uses by the same school district in other contexts, and its perceived cost effectiveness when staffing constraints make increased supervision by personnel infeasible.

D. **Sexual Harassment Laws (Employment)**: School Districts have an affirmative duty to take prompt remedial action to address sexual harassment and are required to take reasonable steps to prevent harassment from occurring. As technological means such as e-mail provide employees with another means to harass other employees, districts are under increased pressure to monitor e-mail communications in order to prevent or respond to inappropriate communications.

## IV. RELEVANT LEGAL AUTHORITY:

A. **Federal Electronic Communications Privacy Act (1986)**:

1. **Scope of the ECPA:**

a. The Federal Electronic Communications and Privacy Act (ECPA) regulates oral and wire communications. The ECPA's protections extend not only to "basic" wire, oral, and written communications, but also to newer means of communications, i.e. electronic mail, voice mail and bulletin boards, computer-to-computer communications, and remote computer services.

The ECPA applies to "aural" or "electronic" communications. Therefore, whether or not a particular video surveillance system includes audio surveillance may be a key issue in determining whether or not an employer will be bound or liable under the ECPA. For example, in United States v. Torres, 751 F.2d 875, 884-85 (7th Cir. 1984), the court recognized that silent videotaping does not fall within the letter of the ECPA. Similarly, in Thompson v. Johnson County Community College, 930 F. Supp. 501 (D.C. Kan., 1996), a Federal District Court in Kansas ruled, as a matter of law, that a defendant community college was entitled to summary judgment because silent video surveillance falls outside the scope of the ECPA.

b. The ECPA covers two types of electronic communications:

(1) In-transit communications.

(2) Stored communications.

c. The ECPA provides for a civil cause of action.

2. **Interception of "In-transit" Electronic Communications.**

The ECPA generally prohibits the unauthorized interception of electronic communications. However, the ECPA does contain exceptions to this general rule:

a. The business use exception. This exception allows employers to monitor telephone calls if the monitoring is done for a legitimate business purpose.

b. The prior consent exception. This exception allows employers to intercept or record communications between employees if any party to the conversation has consented to its interception.

c. The reasonable expectation of noninterception exception. An individual alleging an unlawful interception of oral communication must show that they had a reasonable expectation of noninterception of such communications.

3. **Access to "Stored" Communications**.

The ECPA also prohibits unauthorized access to stored wire and electronic communications, including stored messages in voice mail, e-mail and internet accounts. There are exceptions to this ECPA provision as well:

a. The provider exception: The "entity providing the electronic communications service" to the employee is exempted from this prohibition against access and disclosure of stored communications.

Example: In Bohach v. The City of Reno, 932 F. Supp. 1232 (D. Nev. 1996), the defendant employer, the City of Reno Police Department, provided its employees with a completely "private" or "closed" communications system, which it owned and operated. In that case, the court considered the city the "provider," exempting the city from the ECPA, and allowing the city to access its employees' electronic communications. However, in employment situations where an employer simply contracts with an outside service, such as AT&T, CompuServe or MCI Mail to provide e-mail, voice mail and Internet access for its employees, the employer may not be considered a "provider" of the service.

The officers under investigation filed a lawsuit claiming violation of their Fourth Amendment right to privacy and various federal wiretapping statutes.

The court held that: (a) the officers did not have a reasonable expectation of privacy because the officers knew that their messages were recorded and logged on the department's network n the ordinary course of the department's business (messages were recorded "for a variety of reasons: to make sure that their dispatches are accurate, to verify information and to keep a log of emergency and non-emergency calls"); (b) there was no unlawful interception in violation of the ECPA because the pager messages were not "intercepted" at the time of

transmission, because the system on which the pages operated simply forwarded the message through a computer system; the messages were only later recorded and stored on the department's computer system for logging and archival purposes; and (c) the retrieving of stored messages did not violate the ECPA because the statute does not prohibit the retrieval of messages from a supplier's own system (the department supplied and maintained the system, so the department could do what it wished with the recorded messages).

b. Consent by the user. Consent may be procured from employees explicitly, or implicitly through policies.

Example, Briggs v. American Air Filter Co., 630 F.2d 414 (5th Cir. Ga. 1980): an employee brought a claim for invasion of privacy where the employer recorded workplace phone conversations. The court upheld the employer's action because the recording was done on an extension and because the specific purpose of listening was business related: to ascertain the employee was only using the phone for business.

**B. Employee Polygraph Protection Act, 29 U.S.C. § 2001 et. seq. (EPPA):**

The EPPA makes it illegal, with limited exceptions, for employers to use lie detector tests. The significant exception is for ongoing investigations involving economic loss or injury to the employer's business where there is a reasonable suspicion of workplace theft, embezzlement, misappropriation, and in certain other cases. U.S.C. § 2006(d). *See* Veazey v. Communications & Cable of Chicago, 194 F.3d 850, 858 (7th Cir. 1999).

Disclosure of test results also is generally prohibited. *But see* Long v. Mango's Tropical Café, 972 F. Supp. 655 (S.D. Fla. 1997) (bar owner who revealed discharged employee's polygraph results after the employee sued did not violate EPPA).

**C. Litigation Involving Privacy Rights And Technology:**

1. **Telephone/Voicemail.**

In Deal v. Spears, 980 F. 2d 1153 (8th Cir. 1992), the defendants owned a store adjacent to their mobile home that shared a phone line with their mobile home. After their store was robbed, the defendants installed a recording device on the phone line in their home to monitor the calls of one of their employees who they suspected of committing the robbery. The employee was warned that due to her excess personal calls they might



BEST COPY AVAILABLE

monitor her calls, but did not inform her of the recording device. The Eighth Circuit Court of Appeals held that the employee did not consent to the monitoring because defendants did not inform the employee that they were monitoring her calls, they merely warned her that they might. The court also held that the defendants did not meet the business exemption because the recording device they used had been purchased at Radio Shack, and therefore, had not been supplied by the phone company.

In Watkins v. L.M. Berry & Company, 704 F.2d 577 (11th Cir. 1983), employee calls were ostensibly monitored to help improve sales techniques. The company had a policy, however, that it would only monitor personal calls long enough to determine that they were personal. The employee brought suit against her employer because it had monitored one of her personal calls in its entirety. The Eleventh Circuit Court of Appeals held that the employer did not meet the business exemption because listening to personal calls was not in the employer's ordinary course of business.

Amati v. City of Woodstock, 176 F.3d 952 (7th Cir. 1999). The court concluded that 63 plaintiffs, whose conversations over a police department telephone line were tape recorded, could not prevail under an invasion of privacy claim.

Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999). Plaintiffs were awarded $160,000 against their supervisor for violation of their privacy when the supervisor surreptitiously tape recorded their conversations. The court held that the plaintiffs had reasonable subjective and objective expectations of privacy, because the employer did not have any policies that cautioned that their conversations might be tape recorded.

2. **E-Mail**.

Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996). Pillsbury maintained an electronic mail system in order to promote better internal communications between its employees. Pillsbury repeatedly assured its employees that any e-mail communications would remain confidential. Pillsbury further assured its employees that such e-mail transmissions could not be intercepted and used by the company as grounds for termination or reprimand. The company intercepted plaintiff's private e-mail messages and terminated him for what it deemed inappropriate and unprofessional comments over the e-mail system. Plaintiff sued for wrongful discharge when it terminated him for transmitting what the company deemed to be inappropriate and unprofessional comments over its e-mail system.

The court granted Pillsbury's motion to dismiss based on its finding that the plaintiff employee did not have "a reasonable expectation of privacy in e-mail communications voluntarily made by [him] to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. In addition, the court noted that "by intercepting such communications, the company is not, as in the case of urinalysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects."

In Harley v. McCoach, 928 F. Supp. 533 (E.D. Pa. 1996), an employer had to defend a lawsuit based on sexual harassment involving the use of e-mail. In addition to a large amount of sexual conduct, the court reviewed an e-mail message sent to Plaintiff identifying her as "Brown Sugar." After the plaintiff complained to her employer, the employer instituted remedial measures, which included removal of e-mail capability from the workplace. Despite the fact that the employer took away e-mail privileges, the court found for the employee.

In Strauss v. Microsoft Corp., 814 F. Supp. 1186 (S.D.N.Y. 1993), one of the defendants sent an e-mail message to all of his staff referring to a female employee as "spandex queen," and referring to himself as president of the "amateur gynecology club." In addition, the same defendant forwarded to a male staff employee an e-mail message containing a news report on Finland's proposal to institute a sex holiday and an e-mail containing a parody of a play entitled "A Girl's Guide to Condoms." Those messages were then forwarded to the plaintiff. Despite the fact that some of the messages were not sent directly to the plaintiff, it was the distribution of the information that the plaintiff was eventually made aware of that led the court to find for the employee.

3. **Internet**.

Key cases involving internet monitoring have involved government workplaces and an employee's Fourth Amendment rights to be protected from unreasonable searches. Whether the monitoring or search is in violation of the employee's Fourth Amendment rights turns on whether the employee had an expectation of privacy. Where the employer has a known policy allowing monitoring, the courts have concluded that the employee does not have a privacy expectation.

United States v. Simons, 206 F.3d 392 (4th Cir. 2000). A former employee was convicted for receiving and possessing child pornography after he had downloaded more than 1,000



BEST COPY AVAILABLE

files that contained pornography. The employee challenged the search of his computer on the grounds that it was an unreasonable search in violation of the Fourth Amendment.

The court concluded that there was no violation because the employee lacked a legitimate expectation of privacy in the files he had downloaded from the internet, because the government had a policy that "clearly stated that FBIS would 'audit, inspect and/or monitor' employees' use of the Internet, including all file transfers, all websites visited, and all e-mail messages, 'as deemed appropriate.'"

Muick v. Glenayre Electronics, -- F.3d --, 2002 WL 181726 (7th Cir. 2002). An employee alleged that the employer violated his Fourth and Fifth Amendment rights (and rights under Illinois law) when it seized his laptop computer at the request of federal agents and held the computer until such time as the government obtained a search warrant to determine whether the employee possessed child pornography. The employer "announced that it could inspect laptops that if furnished for the use of its employees, [the announcement] destroyed any reasonable expectation of privacy that [the employee] might have had ...." Consequently, the employee did not have a federal constitutional cause of action against his employer.

4. **Video Surveillance**.

Video surveillance in public and open spaces is generally permissible. As the court noted in Vega-Rodriquez v. Puerto Rico Telephone Company, 110 F.3d 174 (1st Cir. 1997), "no legitimate expectation of privacy exists in objects exposed to plain view as long as the viewer's presence at the vantage point is lawful." The court stated that an employer may monitor areas that are in plain view within an open work area.

Video surveillance in what are arguably "private" areas may implicate privacy interests. *See, e.g.*, Cramer v. Consolidated Freightways, Inc., 225 F.3d 683 (9th Cir. 2001) (employee could bring a state law claim against its employer where the employer installed two-way mirrors (and video cameras) in its employees' restrooms to facilitate detection of employee drug-users, a use of surveillance equipment that was arguably illegal under California law). *See also*, Doe by Doe v. B.P.S. Guard Services, Inc., 945 F.2d 1422 (8th Cir. 1991) (cause of action was stated where surveillance was made of a dressing room, even though none of the plaintiffs was viewed in state of undress).

In Meche v. Wal-Mart Stores, Inc., 392 So. 2d 544 (1997), employees of a Wal-Mart store brought an invasion of privacy claim. Unbeknownst to the owner of the store, a security guard had placed a video camera in one of the employee unisex restrooms. The

court dismissed that claim because the employees could not establish that any footage was actually taken of any employees using the restroom. The court stated that "at best, we consider the facts herein to have established an attempted invasion of privacy," which is not an actionable claim. The court also dismissed a sexual harassment claim, partly because the bathroom was unisex and the incident was not aimed at any one gender.

## V. NEGLIGENCE THEORIES THAT MAY IMPACT ON SCHOOLS' USE OF MONITORING TECHNOLOGY

**A. Origins Of The Duty**: Courts often cite the Restatement (Second) of Agency as authority for the doctrine of negligent supervision. That section states:

213 Principal Negligent or Reckless

A person conducting an activity through servants or other agents is subject to liability for harm resulting from his conduct if he is negligent or reckless:

1. in giving improper or ambiguous orders or in failing to make proper regulation;

2. in the employment of improper persons or instrumentalities in work involving risk of harm to others;

3. in the supervision of the activities; or

4. in permitting, or failing to prevent, negligent or other tortuous conduct by persons, whether or not his servants or agents, upon premises or with instrumentalities under his control.

**B. Elements**. In order to state a claim for negligent supervision; a plaintiff bears the burden of proving the following elements:

1. The defendant owed a duty to the plaintiff. In general, schools have a duty to exercise reasonable care, in view of all the circumstances, in regulating the actions of individuals who might pose a threat of injury to others.

2. The school district knew or should have known that the individual posed an unreasonable risk and did not address that risk.

a. The plaintiff must prove the school district had actual or constructive knowledge of unfitness or risk.

b. A plaintiff may provide actual knowledge by showing the school district possessed evidence of unfitness (e.g., past performance reviews, disciplinary notices), or by showing the employer personally witnessed behavior that would apprise it of risks.

c. A plaintiff may prove constructive knowledge by showing a reasonable investigation would have alerted the school district to risks posed by another individual of the employee's fitness.

## VI. USE OF TECHNOLOGY TO MONITOR STUDENT AND EMPLOYEE ACTIVITIES:

Relevant decisions indicate that privacy interests may be protected in certain circumstances involving private telephone conversations. However, employee and student use of e-mail and the internet is clearly subject to monitoring. Further, the use of video surveillance in areas that are not subject to special privacy protections (buses, halls, parking lots, playgrounds, and classrooms) is permissible. Consequently, school officials appear to have broad authority to employ such technology to prevent harm to students and employees under their supervision, and may be under increasing pressure to do so to avoid liability exposure under negligence and other theories of law.

The kinds and degree of monitoring that a school district chooses to engage in will, of course, be influenced by school districts' philosophies on privacy, budgetary considerations, and a series of factors deemed relevant to risk analysis. Nevertheless, to the extent that technological monitoring increasingly becomes a practical necessity, certain strategies appear supportable.

### A. E-Mail And Internet Usage Monitoring:

#### 1. <u>Acceptable use policies must</u>:

- ❖ Place employees on notice that e-mail and internet activity will be monitored and is not private.
- ❖ State that monitoring cannot detect all conduct that may violate harassment policies or other rights of staff/students, and therefore that the district depends upon timely reporting by users of the system to prevent such activity.

- ❖ Instruct staff/students on appropriate methods for preserving evidence of offending conduct.
- ❖ Identify conduct that violates acceptable use standards.
- ❖ Provide for remedial measures (including revocation) when violations occur.

2. **Procedures to consider**:

- ❖ Use blocking technology to prevent certain materials or content from being transmitted.
- ❖ Place blocking restrictions on pictorial transmissions.
- ❖ Require passwords for logging on and provide that users must log on only at specified terminals (and when this is not permissible, for check in procedure logging use of another terminal).
- ❖ Use servers that allow for downloading the contents of a particular termination from another location.
- ❖ Provide for spot checks of e-mail messages that do not meet criteria for business usage.
- ❖ Provide for e-mail messages to be transmitted for review when certain address book captions are used and when messages are forwarded containing multiple prior addresses.
- ❖ Establish a SMTP gateway to filter unwanted e-mail before it hits the server or use mailboxes.

**B. Video Cameras:**

- ❖ Camera use may need to be considered in certain areas where supervision cannot reasonably be maintained through the use of personnel:
  - -- School buses
  - -- Hallways that are more remote or low traffic
- ❖ School districts must have a discussion about video surveillance of playgrounds and parking lots which, though more common in certain areas, is not used at all in many schools around the nation. On the one hand, video surveillance can provide general deterrence (though the primary value of most systems is investigative, rather than preventative) and can potentially capture behavior that might otherwise not be detected. On the other hand, video surveillance in these settings is less revealing than many believe (due to the lack of detail that wide field shots provide and the lack of context for recorded events, even for behavior that can be observed), and can actually support liability claims against school

district. Further, video camera systems that will truly deter undesirable behavior tend, at least in the view of some, to be more ominous, raising separate issues concerning the climate that the school district wishes to promote.

- ❖ Decoy cameras should be considered for deterrent effect in circumstances where school districts decide to use video taping.
- ❖ General notice should be given of general video camera usage to maximize their deterrent effect and to act as a hedge against ill-founded claims of invasion of privacy.

**C. Audio Surveillance**:

- ❖ Monitoring incoming calls from the public.

**D. Metal Detectors**:

- ❖ School districts must provide a basis for adopting metal detector strategies as well as procedures for their use. The California Attorney General's office has suggested, e.g., that school officials identify incidents involving weapons or a developing patterns of weapons possession or usage as a predicate for adopting such policies. Such citations will, however, stimulate liability claims if a decision is made not to adopt inspection procedures in response to increased possession and/or usage of firearms. The Synopsis provided by the California Attorney General's office (at 92 Cal. Att'y Gen. Op. 201 (Oct. 6, 1992)), also suggests the following:
  - -- Advance notice of the search;
  - -- Request that students empty their pockets of all metal objects;
  - -- Request a second walk-through when the detector is activated;
  - -- Use a hand held detector to identify the source of the read if a second activation occurs;
  - -- If the activation is not explained, the search may need to be expanded; if no less restrictive means exist, a pat down search may be required;
  - -- For any greater intrusion, the student may be asked to proceed to a private area;
  - -- Any expanded search, such as requests to open purses or backpacks, could be conducted by school officials of the same sex as the students searched.

- School districts must determine whether fixed station and/or hand held metal detectors are to be used.
- Personnel using hand held metal detectors must be trained in equipment operation and in avoiding intrusive behavior that might give rise to privacy claims.
- Use of police officers as part of metal detection strategies should be discussed; such use may be permissible when the officer is acting as a school official, but may constitute an unlawful search (and seized evidence subject to suppression) in other circumstances. *See* People v. Parker, 284 Ill. App. 3d 860, 672 N.E. 2d 813 (1996) (student attempting to enter school turned to leave when he was stopped by a police officer and required to go through a metal detector; the gun that was seized was suppressed). In addition, because school officials' capacity to search in response to a positive metal detector read is not unlimited, employees must have the capacity to respond to high stress situations when students do/do not empty their pockets.

**E. General Risk Management Procedures**

**U.S. Department of Education**
*Office of Educational Research and Improvement (OERI)*
*National Library of Education (NLE)*
*Educational Resources Information Center (ERIC)*

# NOTICE

## Reproduction Basis

| | |
|---|---|
| X | This document is covered by a signed "Reproduction Release (Blanket)" form (on file within the ERIC system), encompassing all or classes of documents from its source organization and, therefore, does not require a "Specific Document" Release form. |
| | This document is Federally-funded, or carries its own permission to reproduce, or is otherwise in the public domain and, therefore, may be reproduced by ERIC without a signed Reproduction Release form (either "Specific Document" or "Blanket"). |